**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF NEW JERSEY**

| | |
|---|---|
| BRIAN D. GRAIFMAN, individually and on behalf of all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>CARECENTRIX, INC.,<br><br>Defendant. | Civil Action No.:<br><br>**CLASS ACTION COMPLAINT**<br><br>**JURY TRIAL DEMANDED** |

Plaintiff Brian D. Graifman ("Plaintiff"), individually and on behalf of all others similarly situated, upon personal knowledge of the facts respectively pertaining to himself and on information and belief as to all other matters, by and through undersigned counsel, hereby bring this Class Action Complaint against defendant CareCentrix, Inc. ("CareCentrix" or the "Defendant").

## I. NATURE OF THE ACTION

1. Plaintiff, individually and on behalf of all others similarly situated, brings this class action on behalf of all persons whose personal information was compromised as a direct result of Defendant's failure to safeguard its patients' highly sensitive medical, personal, and financial information.

2. Contrary to Defendant's promises to maintain that Personal Information in a secure fashion, and despite the fact that the threat of a data breach has been a well-known risk to Defendant, especially due to the valuable and sensitive nature of the data Defendant maintains, Defendant failed to take the reasonable steps to adequately protect the Personally Identifiable Information ("PII") and Protected Health Information ("PHI") of its patients. The data breach was

a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect PII and PHI.

3. Plaintiff and the Class members would not have provided their PII and PHI to Defendant or its agents if Plaintiff and Class members knew that Defendant would fail to ensure that the vendors it used for collection purposes would provide adequate security measures.

4. As a result of Defendant's failure to take reasonable steps to adequately protect the ultra-sensitive PII and PHI of its patients, Plaintiff's and Class members' PII and PHI are now in the hands of thieves.

5. Defendant's failure to implement and follow basic security procedures has resulted in ongoing harm to Plaintiff and Class members who will continue to experience data insecurity for the indefinite future and remain at serious risk of identity theft and fraud that could result in significant monetary loss.

6. Accordingly, Plaintiff seeks to recover damages and other relief resulting from the data breach, including but not limited to, compensatory damages, reimbursement of costs that he and others similarly situated will be forced to bear, and declaratory and injunctive relief to mitigate future harms that are certain to occur in light of the scope of this breach.

## II. JURISDICTION AND VENUE

7. This Court has jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2) ("CAFA"), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000.00, exclusive of interest and costs.

8. The Court has supplemental jurisdiction over Plaintiff's state law claims pursuant to 28 U.S.C. § 1367(a).

9. The Court has personal jurisdiction over Defendant because on or about July 31, 2019 the United State Judicial Panel on Multi-District Litigation has transferred all related matters to this District.

10. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) because a substantial part of the events or omissions giving rise to the conduct alleged in this Complaint occurred in, were directed to, and/or emanated from this District. Venue is additionally proper because the Multi District Litigation Panel has transferred all matters related to the subject matter of this lawsuit to this District.

## III. PARTIES

11. Plaintiff Brian D. Graifman is a resident of New York. On or about August 13, 2016 Plaintiff obtained medical equipment from Landauer Medstar and thereby entrusted Landauer Medstar and its agents with his PII. By letter dated January 24, 2018, American Medical Collection Agency, Inc ("AMCA") informed Plaintiff that it had been retained in connection with a past due amount owed to AMCA's client CareCentrix. It appears that either Landuaer or Plaintiff's health insurer MVP Cigna Healthcare contracted with CareCentrix to perform certain "monitoring services" on Plaintiff's or Plaintiff's insurer's behalf. In connection with that process, CareCentrix was thus entrusted with Plaintiff's PII and PHI.

12. Defendant CareCentrix is incorporated in Delaware and is a health services management company with headquarters at 20 Church Street in Hartford, Connecticut. The Company offers sleep disorder, residential and wound care, risk assessment, medication, and infusion management services.

## IV. FACTUAL BACKGROUND

13. By letter dated July 10, 2019, CareCentrix notified Plaintiff that a collection company

known as AMCA had been the subject of a "data privacy incident" and that the breach (the "Security Breach") may have included Plaintiff's private data which contained Plaintiff's PII and PHI (also referred to herein as "Private Information") which included his first and last name, identify of his medical provider(s) and dates of service (collectivity, the "Data Breach Notification").

14. Further the letter reported that AMCA had informed CareCentrix that on March 20, 2019 it had received notice that the Security Breach was the result of unauthorized access to its systems, possibly its "web payments page." The July 10th Data Breach Notification stated that the breach occurred between August 1, 2018 and March 30, 2019.

15. CareCentrix provides health benefits management services to more than 23 million people by connecting providers and patients through a national network of more than 8,000 credentialed providers throughout the country.[1] It claims to be uniquely "set apart" to provide post-acute care and "support and coordination for patients and their families throughout care transitions, including, among other things, "Home Sleep Services." [2]

16. CareCentrix contracted AMCA for revenue service operations and for collection purposes

17. As a result of the breach of AMCA's systems for a time period estimated to be from August 1, 2018, to March 30, 2019, there was massive theft of private information "from AMCA's corporate "clients." These included CareCentrix as well as Quest Diagnostics, LabCorp, BioReference Laboratories, and Sunrise Laboratories."[3]

---

[1] https://finance.yahoo.com/news/lawsuit-hundreds-employees-health-management-051353574.html(last accessed August 7, 2019).
[2] https://www.carecentrix.com/about-us(last accessed August 7, 2019).
[3] See article appearing in Zero Day, entitled "Data Breach Forces Medical Collector AMCA to file for bankruptcy protection" online at https://www.zdnet.com/article/medical-debt-collector-amca-files-for-bankruptcy-protection-after-data-breach/.(last accessed August 7, 2019).

18. One of these "clients"—CareCentrix—had been providing "monitoring services" in connection with Plaintiff's use of a CPAP device.

19. At all relevant times, CareCentrix promised and agreed to safeguard and protect PII and PHI in accordance with Health Insurance Portability and Accountability Act ("HIPAA") regulations, federal, state and local laws, and industry standards.

20. While CareCentrix had its own Privacy Policy (excerpted below), CareCentrix agreed that it was bound to the privacy and security policies of the Health Care Plans concerning Plaintiff and Class Members and that its Privacy Policy supplemented each Health Care Plan Policy pursuant to CareCentrix's Customer Agreements with those Health Care Plans. (collectively, "Customer Agreements").

21. Under the term "Privacy Policy" on CareCentrix's website, CareCentrix states, in relevant part:

> CareCentrix, Inc. and its current and future affiliates and subsidiaries ("CareCentrix", "we", "our" or "us") collect information from you when you visit and interact with the websites ("Sites"), mobile applications ("Apps"), and other online services that we own and/or operate and that link to this Privacy Policy (collectively, the "Services"). This Privacy Policy does not apply to information collected through other means such as by telephone or in person, although that information may be protected by other privacy policies or agreements.
>
> ***This Privacy Policy explains what information we collect, how we use it, and your choices related to your information. With respect to Protected Health Information (as defined under HIPAA) and other information that we receive from our health plan customers ("Health Plan Customers"), we have entered into agreements with such Health Plan Customers that govern our use of the information (the "Customer Agreements"). The terms of this Privacy Policy supplement the Customer Agreements. However, to the extent that this Privacy Policy conflicts with any applicable Customer Agreement, the Customer Agreement will control. If you are a member under a plan issued by a Health Plan Customer and have questions about the treatment of your Protected Health Information, you should check with the Health Plan Customer.***
>
> This Privacy Policy is incorporated into and made a part of the Terms of Use https://www.carecentrix.com/privacy-policy. Please review our Terms of Use

> because they govern your use of the Services and limit our liability to you. By using our Services, you agree that we may treat your information in the ways we describe in this Privacy Policy. **If you do not agree with any term of this Privacy Policy or the Terms of Use, you may not use our Services.**
>
> (emphasis added).

22. In a separate press release CareCentrix touted its data security. On September 27, 2018 CareCentrix announced "that several of their technology platforms used to store, process, maintain, and transmit customer electronic protected health information (ePHI)* have earned Certified status for information security by HITRUST" that its technology platforms which "store, process and access, maintain and transmit customer ePHI have met key regulatory requirements, industry requirements and are appropriately managing risk."[4]

23. CareCentrix further claimed that meeting the above standards placed it in an "elite" group of organizations that have earned this certification which, according to John Driscoll, CareCentrix's Chief Executive Officer, represented the "gold standard" of security. This certification furthermore demonstrates CareCentrix's commitment to "patient data privacy and safety."

24. These statements were untrue and in stark contrast to the negligent and casual way CareCentrix handed over Plaintiff and the Class and Subclass' PII and PHI to AMCA.

25. Despite the fact AMCA was notified of the data breach on March 20, 2019, CareCentrix did not notify Plaintiff until July 10, 2019.

26. According to FTC policy as set forth in the FTC Press Release dated June 12, 2019, entitled "Data Security Settlement with Service Provider Includes Updated Order Provisions:"

> **If your company uses third-party software or providers, build security into**

[4] See article dated September 27, 2018 contained in "CISTON PR Newswire" appearing online at https://www.prnewswire.com/news-releases/carecentrix-achieves-hitrust-csf-certification-to-manage-risk-improve-security-posture-and-meet-compliance-requirements-300720069.html. (last accessed August 7, 2019).

> **your contracts.** Even if another company's conduct is implicated in a breach, *your* customers' information could be at risk and they'll want to know what *you* did to protect them. As the FTC's publication Start with Security suggests, when entrusting data to third-party service providers, spell out your security expectations, monitor what they're doing on your behalf, and follow websites that report on known vulnerabilities.
>
> **Service providers are accountable for protecting the personal data they collect and store.** ***Even if your operations are behind the scenes, you still may be liable for violations of the law. If you handle sensitive consumer data on behalf of other companies, security should be front and center.*** (emphasis added).[5]

**The Data Breach was a Foreseeable Risk of which Defendant was on Notice**

27. Identity thieves and cyber criminals have targeted the medical industry in the last several years given the treasure trove of ultra-sensitive personal data stored on their systems.

28. The medical industry is rife with examples of hackers targeting users' PII and PHI, including breaches of systems maintained by Anthem, Premera, and St. Joseph Health System, among others, all of which predate the time frame Defendant has identified with regard to the data breach at issue.

29. As early as 2014, the FBI alerted healthcare stakeholders that they were the target of hackers, stating "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[6]

30. To date and based on information and belief, CareCentrix has yet to publicly even acknowledge that third party AMCA, to which it had negligently outsourced and entrusted Plaintiff's and proposed Class and Subclass members confidential PII, had been the subject of a

[5] See press release dated June 12, 2019 appearing online at https://www.ftc.gov/news-events/blogs/business-blog/2019/06/data-security-settlement-service-provider-includes-updated. (last accessed August 8, 2019)

[6] *See "FBI warns healthcare firms they are targeted by hackers",* Reuters (Aug. 20, 2014), *available at* http://www.reuters.com/article/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U201 40820 (last accessed August 7, 2019).

major security and data breach.

31. Defendant's failures are all the more remarkable and glaring in light of its public assurance and boasts contained in paragraphs 20 and 21 above.

**Plaintiff and Class and Subclass Members Were Grievously Harmed by The Data Breach**

32. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[7] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[8]

33. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use identifying data such as Social Security Numbers to open financial accounts, receive government benefits and incur charges and credit in another person's name.[9] As the GAO Report states, this type of identity theft is the most harmful because it often takes some time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

[7] 17 C.F.R. § 248.201 (2013).
[8] *Id.*
[9] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent Is Unknown* (June 2007), United States Government Accountability Office, *available at* https://www.gao.gov/new.items/d07737.pdf (last visited August 7, 2019).

34. Accordingly, identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit.[10]

35. PII and/or PHI is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[11]

36. A study by Experian found that the "average total cost" of medical identity theft is "about $20,000.00" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[12]

37. Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.

38. For all the above reasons, Plaintiff and the Class members have suffered harm; and there is a substantial risk of injury to Plaintiff and the Class members that is imminent and concrete and that will continue for years to come.

39. Plaintiff and Class members are also at risk of imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by their Private Information being placed in the hands of criminals who have already misused such

---

[10] *Guide for Assisting Identity Theft Victims*, Federal Trade Commission, 4 (September 2013), *available at* http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf (last visited August 7, 2019)

[11] GAO Report at 29.

[12] *See Study: Medical identity theft is costly for victims,* CNET (Mar. 3, 2010), *available at* https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed August 7, 2019).

information stolen in the Security Breach via sale of their Private Information (as well as that of Class members') on the Internet black market.

40. Plaintiff has a continuing interest in ensuring that his Private Information is protected and safeguarded from future breaches

41. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendant.

42. The injuries suffered by Plaintiff and Class members as a direct result of the Security Breach include:

a. unauthorized use of their PII and PHI;

b. theft, or threat of theft, of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their PII and PHI;

e. Plaintiff and other members of the Class and Sub-Class, because of loss of their PHI, will be forced to spend additional hours maintaining heightened diligence of all of their medical insurance policies, for fear of acts of identity theft against them and their families;

f. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address an attempt to ameliorate, mitigate and deal with the actual and future consequences of the Security Breach, and the stress, nuisance and annoyance of dealing with all issues resulting from the Security Breach;

g. the imminent and certain impending injury flowing from potential fraud and identity theft posed by current, prior, and future misuse of PII and/or PHI by criminals via the sale of Plaintiff's and Class members' information on the Internet black market;

h. damages to and diminution in value of their PII and PHI entrusted to CareCentrix and the loss of Plaintiff's and Class members' privacy; and

i. the costs of subscribing to, and/or continuing to subscribe to, identity theft protection services.

## V. CLASS ACTION ALLEGATIONS

43. Plaintiff brings this action on behalf of himself and on behalf of two classes – a Nationwide Class and a New York Subclass (together "Classes" or "Class Members") pursuant to the Federal Rule of Civil Procedure 23(b)(2) and (b)(3).

44. The Nationwide Class is defined as follows: All persons in the United States whose PII and PHI was compromised as a result of the data breach referred to in the notification of CareCentrix on or about July 10, 2019, *i.e.* the Data Breach Notification.

45. The New York Subclass is defined as follows: All persons in the State of New York whose PII and PHI was compromised as a result of the data breach referred to in the notification of CareCentrix on or about July 10, 2019*, i.e.* the Data Breach Notification.

46. Excluded from the Class and Subclass is Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

47. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

48. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class and Subclass are so numerous that joinder of all Class members would be impracticable. On information and belief, Class and Subclass members number are in the tens, if not hundreds, of thousands.

49. C**ommonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all Class and Subclass members and predominate over questions affecting only individual Class and Subclass members. Such common questions of law or fact include, *inter alia*:

a. Whether Defendant failed to use reasonable care and commercially reasonable methods to secure and safeguard Plaintiff's and Class and Subclass members' Private Information;

b. Whether Defendant properly implemented its purported security measures to protect Plaintiff's and Class and Subclass members' Private Information from unauthorized capture, dissemination, and misuse;

c. Whether Defendant took reasonable measures to determine the extent of the Security Breach after it first learned of same;

d. Whether Defendant's conduct constitutes breach of an implied contract;

e. Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and Class and Subclass members' Private Information;

f. Whether Defendant was negligent in failing to properly secure and protect Plaintiff's and Class and Subclass members' Private Information;

g. Whether Plaintiff's and the other members of the Class and Subclass are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

50. Defendant engaged in a common course of conduct giving rise to the legal rights

sought to be enforced by Plaintiff, on behalf of himself and other Class and Subclass members. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

51. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the claims of the other Class members because, among other things, all Class and Subclass members were similarly injured through Defendant's uniform misconduct described above and were thus all subject to the Security Breach alleged herein. Further, there are no defenses available to Defendant that are unique to Plaintiff.

52. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate Class and Subclass representative because (1) his interests do not conflict with the interests of the other Class and Subclass members he seeks to represent, (2) he has retained counsel competent and experienced in complex class action litigation, and (3) Plaintiff will prosecute this action vigorously. The Class' and Subclass' interests will be fairly and adequately protected by Plaintiff and his counsel.

53. **Insufficiency of Separate Actions—Federal Rule of Civil Procedure 23(b)(1).** Absent a representative class action, members of the Class and Subclass would continue to suffer the harm described herein, for which they would have no remedy. Even if separate actions could be brought by individual consumers, the resulting multiplicity of lawsuits would cause undue hardship and expense for both the Court and the litigants, as well as create a risk of inconsistent rulings and adjudications that might be dispositive of the interests of similarly situated consumers, substantially impeding their ability to protect their interests, while establishing incompatible standards of conduct for Defendant. The Class and Subclass thus satisfy the

requirements of Fed. R. Civ. P. 23(b)(1).

54. **Injunctive Relief – Federal Rule of Civil Procedure 23(b)(2).** Defendant has acted and/or refused to act on grounds that apply generally to the Class and Subclasses, making injunctive and/or declaratory relief appropriate with respect to the classes under Fed. R. Civ. P. 23(b)(2).

55. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other Class and Subclass members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for Class members to individually seek redress for Defendant's wrongful conduct. Even if Class and Subclass members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

## VI. CAUSES OF ACTION

### COUNT I
### NEGLIGENCE
### (On Behalf of the Nationwide Class Against Defendant)

56. Plaintiff re-alleges and incorporates by reference all paragraphs as if fully set forth herein.

57. As an agent of the Health Care Plans for whom it acted, including the Health Care Plans of Plaintiff and Class Members, CareCentrix obtained from Plaintiff and Class members their non-public, sensitive PII and PHI to obtain medical services, which it provided to AMCA for billing purposes.

58. Defendant has (and continues to have) a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting their PII and PHI. Defendant also had (and continues to have) a duty to use ordinary care in activities from which harm might be reasonably anticipated (such as in the storage and protection of PII and PHI within its possession, custody and control, and that of their vendors).

59. Defendant's duty to use reasonable security measures arose as a result of the fact that: (i) CareCentrix is contractually bound by the Customer Agreements with the Health Care Plans of the Plaintiff and the Class requiring Defendant to maintain, securely, privately, and confidentially the PII and PHI of Plaintiff and the Class, to which Class members are third party beneficiaries; (ii) Defendant is an agent of the Health Care Plans of Plaintiffs and Class and Subclass members; and (iii) the relationship that existed between CareCentrix and patients' said Health Care Plan is recognized by laws including, but not limited to, the Health Insurance Portability and Accountability Act ("HIPAA"). Only Defendant was in a position to ensure that its systems and the systems to which it entrusted this information were sufficient to protect Plaintiff and the Class and Subclass members from the harm of a data breach.

60. Defendant violated these standards and duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class and Subclass members' PII and PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems

to safeguard and protect PII and PHI entrusted to it – including Plaintiff's and Class members' PII and PHI. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII and PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems and to monitor the same of its vendors to whom it gave such Private Information, would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII and PHI.

61. Defendant, by and through its negligent actions, inaction, omissions, and want of ordinary care, unlawfully breached their duties to Plaintiff and Class members by, among other things, failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII and PHI within their possession, custody and control.

62. Defendant, by and through its negligent actions, inactions, omissions, and want of ordinary care, further breached their duties to Plaintiff and Class members by failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit their processes, controls, policies, procedures, protocols, and software and hardware systems for complying with the applicable laws and safeguarding and protecting their PII and PHI.

63. But for Defendant's negligent breach of the above-described duties owed to Plaintiff and Class members, their PII and PHI would not have been released, disclosed, and disseminated without their authorization.

64. Plaintiff's and Class members' PII and PHI was transferred, sold, opened, viewed, mined and otherwise released, disclosed, and disseminated to unauthorized persons without their authorization as the direct and proximate result of Defendant's failure to design, adopt, implement, control, direct, oversee, manage, monitor and audit their processes, controls, policies, procedures

and protocols for complying with the applicable laws and safeguarding and protecting Plaintiff's and Class members' PII and PHI**.**

65. Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused this data breach constitute negligence.

66. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the data breach, Plaintiff and Class members have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing medical policies and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

**COUNT II**
**BREACH OF IMPLIED CONTRACT**
**(On Behalf of the Nationwide Class Against Defendant)**

67. Plaintiff re-alleges and incorporates by reference all paragraphs as if fully set forth herein.

68. Defendant provided Plaintiff and Class members with an implied contract to protect and keep private their PII and PHI.

69. Plaintiff and Class members would not have provided or allowed their PII and PHI to be provided to Defendant or its subsidiaries or contractors, but for Defendant's implied promises to safeguard and protect their information.

70. Plaintiff and Class members performed their obligations under the implied contract when they provided their PII and PHI to obtain necessary medical devices or services and when they paid for the service provided by CareCentrix.

71. Defendant breached the implied contracts with Plaintiff and Class members by failing to protect and keep private their PII and PHI.

72. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and Class members have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing medical policies and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

## COUNT III
## VIOLATION OF NEW YORK CONSUMER LAW FOR DECEPTIVE ACTS AND PRACTICES AND FALSE ADVERTISING OR NEW YORK GEN. BUS. LAW § 349
**(On Behalf of the New York Subclass only)**

73. Plaintiff individually and on behalf of the other New York Subclass members, re-alleges the allegations contained in all paragraphs as though fully set forth herein.

74. Defendant's practices, acts, policies and course of conduct, as described herein, including making representations that they possessed sufficient security to maintain the privacy of such PII and PHI and that CareCentrix would adhere to the privacy and security requirements of the Customer Agreements, were intended to induce, and did induce, Plaintiff and the New York Subclass to allow their PII and PHI to be provided their sensitive PII to Defendant or its

agents.

75. Plaintiff and the New York Subclass members never would have provided their sensitive and personal PII if they had been told or knew that Defendant CareCentrix and its sub-vendors failed to maintain sufficient security to keep such PII from being hacked and taken by others, or that Defendant's failed to ensure that such information would be maintained in encrypted form.

76. Defendant's practices, acts, policies and course of conduct are actionable in that:

a. Defendant actively and knowingly misrepresented or omitted disclosure of material information to Plaintiff and the New York Subclass at the time they provided such PII and PHI information that Defendant or its agents and vendors did not have sufficient security or mechanisms to protect PII and PHI; and

b. Defendant failed to give adequate warnings and notices, failed to take an adequate investigation, and failed to conduct due diligence of AMCA regarding the defects and problems with its system(s) of security systems that it maintained to protect Plaintiff's and the New York Subclass's PII. Defendant possessed prior knowledge of the inherent defects in its' and AMCA's systems and failed to address the same or to give adequate and timely warnings that there had been a Security Breach and hacking episodes had occurred.

77. The aforementioned conduct is and was deceptive, false, and fraudulent and constitutes an unconscionable commercial practice in that Defendant has, by the use of false or deceptive statements and/or knowing intentional material omissions, misrepresented and/or concealed the defective security system they maintained and failed to reveal the Security Breach timely and adequately.

78. Members of the public were deceived by and relied upon Defendant's affirmative misrepresentations and failures to disclose.

79. Such acts by Defendant are and were deceptive acts or practices which are and/or were, likely to mislead a reasonable consumer providing their PII and PHI to Defendant. Said deceptive acts and practices aforementioned are material. The requests for and use of such PII and PHI materials in New York and concerning New York residents and/or citizens was a consumer-oriented act and thereby falls under the New York consumer fraud statute, General Business Law § 349 and 350.

80. Defendant's wrongful conduct caused Plaintiff and the New York Subclass to suffer a consumer-related injury by causing them to incur substantial expense for protection from misuse of the PII materials by third parties and placing Plaintiff and the New York Subclass at serious risk for monetary damages.

81. In addition to or in lieu of actual damages, because of the injury, Plaintiff and the New York Subclass seek statutory damages for each injury and violation which has occurred.

**COUNT IV**
**VIOLATION OF NEW YORK'S DATA BREACH LAWS – DELAYED NOTIFICATION**
**(N.Y. Gen. Bus. Law § 899-aa)**
**(On Behalf of the New York Subclass only)**

82. Plaintiff individually and on behalf of the other New York Subclass members, re-alleges the allegations contained in all paragraphs as though fully set forth herein.

83. Section 899-aa(3) of the New York General Business Law requires any "person or business which maintains computerized data which includes private information which such person or business does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information

was, or is reasonably believed to have been, acquired by a person without valid authorization."

84. The security breach notification shall be directly provided to the affected persons by: (a) written notice; (b) electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the person or business who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction; (c) telephone notification provided that a log of each such notification is kept by the person or business who notifies affected persons; or (d) substitute notice, if a business demonstrates to the state attorney general that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or such business does not have sufficient contact information. N.Y. Gen. Bus. Law § 899-a (5).

85. The Security Breach described herein this Complaint constitutes a "breach of the security system" of Defendant and its agent AMCA.

86. As alleged above, Defendant unreasonably delayed informing Plaintiff and the New York Subclass about the Security Breach, affecting the confidential and non-public Private Information of Plaintiff and the New York Subclass after Defendant knew the Security Breach had occurred. AMCA learned of the breach on March 20, 2019 and CareCentrix did not notify Plaintiff until July 10, 2019.

87. Defendant failed to disclose to Plaintiff and the New York Subclass, without unreasonable delay and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, Private Information when Defendant knew

or reasonably believed such information had been compromised.

88. Defendant's ongoing business interests gave it incentive to conceal the Security Breach from the public to ensure continued revenue.

89. Upon information and belief, no law enforcement agency instructed Defendant that notification to Plaintiff and the New York Subclass would impede Defendant's investigation.

90. As a result of Defendant's violation of New York law, Plaintiff and the New York Subclass were deprived of prompt notice of the Security Breach and were thus prevented from taking appropriate protective measures securing identity theft protection, or requesting a credit freeze. These measures would have prevented some or all of the damages the Plaintiff and the New York Subclass suffered because their stolen information would not have any value to identity thieves.

91. As a result of Defendant's violation of New York law, Plaintiff and the New York Subclass have suffered incrementally increasing damages separate and distinct from those simply caused by the breaches themselves.

92. Plaintiff and the New York Subclass seek all remedies available under New York law, including, but not limited to, damages the Plaintiff and the New York Subclass suffered as alleged above, as well as equitable relief.

## VII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of all claims so triable.

## VIII. REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Classes proposed in this Complaint, respectfully requests that the Court enter judgment against Defendant, as follows:

A. Declaring that this action is a proper class action, certifying the Class and Subclass as requested herein, designating Plaintiff as Class and Subclass Representative, and appointing Class Counsel as requested in Plaintiff's anticipated Motion for Class Certification;

B. Ordering Defendant to pay actual damages to Plaintiff and the other members of the Class and Subclass;

C. Ordering Defendant to pay punitive damages, as allowable by law, to Plaintiff and the other members of the Class and Subclasses;

D. Ordering Defendant to pay attorneys' fees and litigation costs to Plaintiff and their counsel;

E. Ordering Defendant to pay equitable relief, in the form of disgorgement and restitution, and injunctive relief as may be appropriate;

F. Ordering Defendant to pay both pre- and post-judgment interest on any amounts awarded; and

G. Ordering such other and further relief as may be just and proper.

Date: August 9, 2019

Respectfully submitted,

*/s/ Howard T. Longman*

Howard T. Longman
**STULL, STULL, & BRODY**
354 Eisenhower Parkway, Suite 1800
Livingston, New Jersey 07039
Tel: 973 994 2315
Fax:973 994 2319
Hlongman@ssbny.com

Jay I. Brody, Esq.
**KANTROWITZ, GOLDHAMER, & GRAIFMAN, P.C.**
210 Summit Avenue
Montvale, New Jersey 07645
Tel: (201) 391-7000

Melissa R. Emert
**STULL, STULL, & BRODY**
6 East 45th Street
New York, NY 10017
Tel.: (212) 687-7230
Fax: (212) 490-2022
memert@ssbny.com

***Attorneys for Plaintiff and the proposed Class and Subclass***

* *pro hac vice* application forthcoming